MATH 6370, LECTURE 13
ELLIPTIC CURVES III
APRIL 16

GORDAN SAVIN

Let p be an odd prime $p \equiv 3 \pmod 4$. Then p stays prime in the ring of gaussian integers. The ray class field attached to the ideal (p^n) has the Galois group isomorphic

$$(\mathbb{Z}[i]/p\mathbb{Z}[i])^\times/\mu_4$$

which has order

$$\frac{1}{4}(p^2-1)p^{2(n-1)}.$$

This field is obtained by adjoining squares of x-coordinate of points P on the curve $y^2 = x^3 - x$ such that $p^n \cdot P = O$. We shall partially prove this by checking that the degree of extension is correct. To that end we need general polynomials for $m \cdot P$. Define a sequence of polynomials

$$\psi_1 = 1,\ \psi_2 = 2y,\ \psi_3 = 3x^4 - 6x^2 - 1,\ \psi_4 = 4y(x^6 - 5x^4 - 5x^2 + 1)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m - \psi_{m-1}\psi_{m+1}^3$$

$$2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

Let

$$\phi_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}$$

$$4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.$$

We now need the following theorem, the first two bullets are easy to check.

Theorem 0.1. *Then*

- $\psi_m, \phi_m, y^{-1}\omega_m$, *for m odd ,and* $(2y)^{-1}\psi_m, \phi_m, \omega_m$, *for m even, are polynomials in* $\mathbb{Z}[x, y^2]$. *Substituting $y^2 = x^3 - x$ we may consider them as polynomials in* $\mathbb{Z}[x]$.
- *Considering ψ_m^2 and ϕ_m as polynomials in x,*

$$\phi_m = x^{m^2} + \dots$$

$$\psi_m^2 = m^2 x^{m^2-1} + \dots$$

- *If P is a point on $y^2 = x^3 - x$, then*

$$m \cdot P = \left(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}\right).$$

Thus, for m odd, non-trivial solutions of $m \cdot P = O$ are found by finding $(m^2-1)/2$ roots of $\psi_m(x)$ each of which will give two points $\pm P$ in m-torsion. For m odd, it is easy to check, by induction on m, that $\psi_m(0) = \pm 1$. Hence

$$\psi_m(x) = \pm m x^{(m^2-1)/2} + \dots \pm 1.$$

Since solutions of $p^{n-1} \cdot P = O$ are a subset of solutions of $p^n \cdot P = O$, the polynomial $\psi_{p^{n-1}}(x)$ divides $\psi_{p^n}(x)$. Using Gauss lemma

$$\Phi_{p^n}(x) = \frac{\psi_{p^n}(x)}{\psi_{p^{n-1}}(x)} = \pm p x^{\frac{(p^2-1)}{2} p^{2(n-1)}} + \ldots \pm 1 \in \mathbb{Z}[x].$$

Lemma 0.2. *If* $p \equiv 3 \pmod 4$ *then* $\Phi_{p^n}(x) \equiv \pm 1 \pmod p$.

Proof. The lemma states that $\Phi_{p^n}(x)$ has no roots mod p, in other words the elliptic curve considered modulo p has no primitive solutions to $p^n \cdot P = O$. So we need to prove that the curve has no p-torsion. Reducing ψ_p modulo p we get a polynomial of degree less than $(p^2-1)/2$ so the p torsion can only be trivial (what we want) or $\mathbb{Z}/p\mathbb{Z}$. How do we eliminate the latter? If the p-torsion is $\mathbb{Z}/p\mathbb{Z}$ then the complex multiplication action on the torsion gives a ring homomorphism

$$\mathbb{Z}[i] \to \mathrm{End}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z},$$

clearly surjective, since $1 \mapsto 1$. Now i goes to a square root of -1, but there is no such element in $\mathbb{Z}/p\mathbb{Z}$ since $p \equiv 3 \pmod 4$. □

We remark that an elliptic curve in a positive characteristic p is called super singular if it has no p-torsion. Thus we proved that $y^2 = x^3 - x$ is super singular for $p \equiv 3 \pmod 4$. Going back to our problem, the polynomial $\Phi_{p^n}(x)$ is irreducible by the Eisenstein's criterion. Observe that $\psi_m(x)$ are even polynomials for all odd m. Thus Φ_{p^n} is an irreducible polynomial in x^2 of degree $\frac{1}{4}(p^2-1)p^{2(n-1)}$, over $\mathbb{Q}(i)$, proving that the degree if the extension is at least what was stated.

Of corse, we can get even a larger extension of $\mathbb{Q}(i)$ by adjoining roots of $\Phi_{p^n}(x)$, instead of their squares. However, roots of the even polynomial $\Phi_{p^n}(x)$ come in pairs $\pm\alpha$ so this polynomial is not separable mod 2. Thus, it seems that the extension generated by coordinates of p^n-torsion points will generate an abelian extension of with the Galois group $(\mathbb{Z}[i]/p^n\mathbb{Z}[i])^\times$ but it will be ramified at 2 and p.